IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

CANDACE COOPER-LEONARD, *individually and on behalf of all others similarly situated*, Plaintiff, v. WELLTOK, INC., VIRGIN PULSE, INC., SUTTER HEALTH, and PROGRESS SOFTWARE CORPORATION, Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Candace Cooper-Leonard ("Plaintiff") brings this Class Action Complaint, individually and on behalf of all others similarly situated (the "Class"), against Defendants Welltok, Inc. ("Welltok"), Virgin Pulse, Inc. ("Virgin Pulse"), Sutter Health ("Sutter Health"), and Progress Software Corporation ("PSC") (collectively, "Defendants") and alleges as follows, based upon information and belief, investigation of counsel, and the personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach where unauthorized third-party criminals retrieved and exfiltrated highly-sensitive consumer data belonging to Plaintiff and more than 845,000 Class Members (the "Data Breach"), via a security vulnerability in PSC's software program, MOVEit, which is used by Welltok—a Virgin Pulse company and vendor to Sutter Health—to operate an online contact-management platform.[1] After learning of the Data Breach, Defendants waited nearly three months to notify affected individuals.[2]

[1] *See* Brandon Downs, *Sutter Health announces ransomware attack that exposed personal information of patients*, CBS NEWS SACRAMENTO (Nov. 10, 2023), https://www.cbsnews.com/sacramento/news/sutter-health-announces-ransomware-attack-that-exposed-personal-information-of-patients/.
[2] *See* Data Breach Notice, **Exhibit A**.

2. Defendant Welltok is a software company owned by Defendant Virgin Pulse. Welltok operates an online contact-management platform that enables its healthcare clients, including Defendant Sutter Health, to provide patients with important notices and communications.[3] As part of its business, Defendant Welltok acquires, collects, and stores patients' sensitive personally identifying information ("PII") and protected health information ("PHI") (collectively, "Private Information") from and on behalf of its healthcare clients.

3. Defendant Virgin Pulse advertises itself as "the world's #1 health, wellbeing and navigation platform."[4] Virgin Pulse says it "operate[s] at the intersection of people and data, using a digital platform to gain true human insights and inspire action for the benefit of individuals and organizations."[5] As part of its business, Defendant Virgin Pulse acquires, collects, and stores patients' Private Information.

4. Defendant PSC is a provider of file transfer software and advertises itself as an "experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely."[6]

5. According to Defendant Welltok, the Private Information compromised in the Data Breach included: patient names, dates of birth, addresses, telephone numbers, email addresses, Social Security numbers, Medicare/Medicaid ID numbers, health insurance information, healthcare provider names, treatment cost information, and treatment information or diagnosis.[7]

---

[3] *See* SUTTER HEALTH, *Sutter Health Vendor Reports Patient Information Incident* (Nov. 3, 2023), https://vitals.sutterhealth.org/sutter-health-vendor-reports-patient-information-incident/.
[4] VIRGIN PULSE, https://www.virginpulse.com/ (last visited Dec. 11, 2023).
[5] VIRGIN PULSE, *About Us*, https://www.virginpulse.com/about-us/ (last visited Dec. 11, 2023).
[6] PROGRESS, https://www.progress.com/company (last visited Dec. 9, 2023).
[7] *See* SUTTER HEALTH, *Sutter Health Vendor Reports Patient Information Incident* (Nov. 3, 2023), https://vitals.sutterhealth.org/sutter-health-vendor-reports-patient-information-incident/.

6. Defendant Welltok claims that it takes "the security of personal information in [its] care very seriously."[8] Defendant Virgin Pulse also professes that it is "committed to protecting [patient] rights and [patient] privacy[,]"[9] and Defendant Sutter Health likewise claims to be "committed to respecting [patients'] right to privacy."[10]

7. Despite these outward assurances, Defendants failed to adequately safeguard Plaintiff's and Class Members' highly sensitive Private Information, which they collected, stored, and maintained. Specifically, Defendants Welltok, Virgin Pulse, and Sutter Health used Defendant PSC's MOVEit software to store and transfer the Private Information of Plaintiff and Class Members, and this Private Information was compromised as a result of a security vulnerability in the MOVEit software.

8. It is reported that the Data Breach was carried out by notorious Russia-linked ransomware syndicate Cl0p.[11]

9. Based on the notice posted on its website, Defendant Welltok admits that Plaintiff's and Class Members' Private Information was accessed and compromised by an unauthorized third party.[12] Defendant Sutter Health admits, in the notice posed on its website, that approximately 845,441 Sutter Health patients were impacted by the Data Breach.[13]

---

[8] *Id.*
[9] VIRGIN PULSE, *Privacy Notice*, https://www.virginpulse.com/privacy-notice/ (last visited Dec. 11, 2023).
[10] SUTTER HEALTH, *Your Privacy*, https://www.sutterhealth.org/privacy (last visited Dec. 11, 2023).
[11] Stefanie Schappert, *Cl0p dumps all MOVEit victim data on clearnet, threat insiders talk ransom strategy*, CYBERNEWS (Aug. 18, 2023) (updated November 2023), https://cybernews.com/security/clop-publish-all-moveit-victim-ransom-data-clearweb/.
[12] *See* WELLTOK, *Notice of Data Privacy Event*, https://welltoknotice.wpenginepowered.com/?page_id=23 (last visited Dec. 11, 2023).
[13] *See* SUTTER HEALTH, *Sutter Health Vendor Reports Patient Information Incident* (Nov. 3, 2023), https://vitals.sutterhealth.org/sutter-health-vendor-reports-patient-information-incident/.

10. Defendants owed a non-delegable duty to Plaintiff and Class Members to implement reasonable and adequate security measures to protect their Private Information. Yet, Defendants Welltok, Virgin Pulse, and Sutter Health maintained and shared the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on computer systems in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants Welltok, Virgin Pulse, and Sutter Health, and they were therefore on notice that failing to take steps necessary to ensure their vendors, including Defendant PSC, properly safeguarded Plaintiff's and Class Members' Private Information from those risks left the Private Information in a vulnerable condition.

11. Plaintiff's and Class Members' Private Information was compromised due to Defendants' negligent and/or careless acts and omissions and Defendants' failure to reasonably and adequately protect Plaintiff's and Class Members' Private Information.

12. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including: opening new financial accounts and taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' Private Information to target other phishing and hacking intrusions, using Class Members' Private Information to obtain government benefits, and filing fraudulent tax returns using Class Members' Private Information.

13. As a result of the Data Breach, Plaintiff and Class Members face a substantial risk of imminent and certainly impending harm, heightened here by the loss of Social Security numbers, a class of Private Information which is particularly valuable to identity thieves. Plaintiff and Class Members have and will continue to suffer injuries associated with this risk, including

but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

14. This risk is even more pronounced given the extended amount of time that lapsed between when the Data Breach occurred, when Defendants reportedly determined Plaintiff's and Class Members' Private Information was compromised, and when Defendants actually notified Plaintiff and Class Members about the Data Breach.

15. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

16. Accordingly, Plaintiff brings this action against Defendants, seeking redress for Defendants' unlawful conduct and asserting claims for: (i) negligence; (ii) breach of implied contract; (iii) unjust enrichment; (iv) bailment; and (v) breach of fiduciary duty. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendants' data security systems, policies, and practices, future annual audits, and adequate credit monitoring services funded by Defendants.

THE PARTIES

17. Plaintiff Candace Cooper-Leonard is a natural person, resident, and citizen of the State of California, residing in Placer County.

18. Defendants obtained and continue to store and maintain Plaintiff's Private

Information. Defendants owe Plaintiff a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of Defendants' inadequate data security practices, which resulted in the Data Breach.

19. Plaintiff received a notice letter dated October 31, 2023 from Defendant Welltok, stating that an unauthorized party accessed her Private Information.

20. Defendant Welltok, Inc. is a Delaware corporation headquartered in Colorado and Rhode Island, with a principal place of business located at 75 Fountain Street, Suite 310, Providence, Rhode Island 02902, and a registered agent located at 1900 W. Littleton Boulevard, Littleton, Colorado 80120.

21. Defendant Virgin Pulse, Inc. is a Delaware corporation headquartered in Rhode Island, with a principal place of business located at 75 Fountain Street, Suite 310, Providence, Rhode Island 02902.

22. Defendant Sutter Health is a California nonprofit corporation headquartered in Sacramento, California, with a principal place of business located at 2710 Gateway Oaks Drive, Sacramento, California 95833.

23. Defendant, Progress Software Corporation, is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803.

JURISDICTION AND VENUE

24. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff, and at least one member of the putative Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 putative

class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

25. This Court has general personal jurisdiction over Defendants because Defendants operate in and direct commerce at this District.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant PSC's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendants have harmed Class Members residing in this District.

DEFENDANTS' BUSINESSES

27. Defendant Welltok is a software company that works with health plan providers and manages communications with their subscribers through its platform. Welltok claims to "deliver[] the healthcare industry's leading consumer activation platform."[14] Welltok is owned by Defendant Virgin Pulse and is a vendor and business associate of Defendant Sutter Health.

28. Defendant Virgin Pulse is a software company that offers services in employee engagement, productivity, health, and workplace wellness. Virgin Pulse claims to "impact[] over 100 million people across 190 countries by helping Fortune 500, national health plans and many other organizations change lives – and businesses – for good."[15] Virgin Pulse acquired Defendant Welltok in 2021.[16]

29. Defendant Sutter Health is a nonprofit corporation that "provide[s] coordinated care to more than 3 million Californians."[17]

---

[14] WELLTOK, https://welltoknotice.wpenginepowered.com/ (last visited Dec. 11, 2023).
[15] VIRGIN PULSE, *About Us*, https://www.virginpulse.com/about-us/ (last visited Dec. 11, 2023).
[16] *Virgin Pulse completes acquisition of Welltok, expanding health engagement capabilities for employers, payers and health systems*, VIRGIN PULSE (Nov. 10, 2021), https://international.virginpulse.com/press-releases/virgin-pulse-completes-acquisition-of-welltok-expanding-health-engagement-capabilities-for-employers-payers-and-health-systems/.
[17] Sutter Health, *What is Sutter Health*?, https://www.sutterhealth.org/about/what-is-sutter-health

30. On information and belief, in the ordinary course of its business of providing services, Defendants collect, store, and maintain the Private Information of consumers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number or taxpayer identification number;
- Financial and/or payment information;
- Health billing information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information;
- Health information;
- Other information that Defendants may deem necessary to provide services and care.

31. Additionally, Defendants may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family members.

32. Because of the highly sensitive and personal nature of the information Defendants acquire and store with respect to consumers and other individuals, Defendants, upon information and belief, promise to, among other things: keep Private Information private; comply with financial services industry standards related to data security and Private Information, including

(last visited Dec. 11, 2023).

FTC guidelines; inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Plaintiff and Class Members obtain from Defendant and provide adequate notice to individuals if their Private Information is disclosed without authorization.

33. As a HIPAA covered business entities, Defendants Welltok, Virgin Pulse, and Sutter Health are required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI, as in the case of the Data Breach complained of herein.[18]

34. However, Defendants Welltok, Virgin Pulse, and Sutter Health did not maintain adequate security to protect their systems from infiltration by cybercriminals, and they waited nearly three months to publicly disclose the Data Breach to consumers.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

36. Yet, contrary to Defendants' representations, Defendants failed to implement adequate data security measures, as evidenced by Defendants' admission of the Data Breach, which affected more than 845,000 customers of Defendant Sutter Health.

[18] *See* SUTTER HEALTH, *Privacy Policy*, https://www.sutterhealth.org/privacy/privacy-policy (last visited Dec. 11, 2023).

Defendants are Covered Entities Subject to HIPAA

37. Defendants Welltok, Virgin Pulse, and Sutter Health are all HIPAA covered entities, providing services to millions of patients annually via their hospital and medical practice clients. As a regular and necessary part of their businesses, Defendants Welltok, Virgin Pulse, and Sutter Health collect and store the highly sensitive Private Information of patients. As covered entities, Defendants are required under federal and state law to maintain the strictest confidentiality of the Private Information they acquire, receive, collect, and store. Defendants are further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

38. Due to the nature of Defendants' businesses, which includes providing a range of services to health care clients, including obtaining, storing, and maintaining electronic health records, Defendants would be unable to engage in their regular business activities without collecting and aggregating Private Information that they know and understand to be sensitive and confidential.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants Welltok, Virgin Pulse, and Sutter Health assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

40. Plaintiff and Class Members are or were patients, or are the executors or surviving spouses of patients, whose Private Information was maintained by Defendants Welltok, Virgin Pulse, and Sutter Health and directly or indirectly entrusted Defendants with their Private Information.

41. Plaintiff and Class Members relied on Defendants Welltok, Virgin Pulse, and Sutter Health to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and healthcare purposes, and to prevent unauthorized disclosures of Private Information. Plaintiff and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep that Private Information confidential.

42. As described throughout this Complaint, Defendants Welltok, Virgin Pulse, and Sutter Health did not reasonably protect, secure, or store Plaintiff's and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that they knew or should have known were insufficient to reasonably protect the highly sensitive Private Information that they maintained. Consequently, cybercriminals circumvented Defendants' security measures, resulting in a significant data breach.

THE DATA BREACH AND NOTICE LETTER

43. According to notices posted on Defendant Welltok's website,[19] Defendant Sutter Health's website,[20] and an October 31, 2023 notice letter sent to Plaintiff Cooper-Leonard by Welltok on behalf of Sutter Health (the "Data Breach Notice"), Defendant Welltok uses software made by Defendant PSC (MOVEit), which was subject to a cybersecurity attack that allowed unauthorized parties to access and compromise Plaintiff and Class Members' Private Information between May 28 and 29, 2023.[21]

44. Defendant Welltok used the MOVEit software for transferring large datasets across

[19] WELLTOK, https://welltoknotice.wpenginepowered.com/ (last visited Dec. 11, 2023).
[20] SUTTER HEALTH, *Sutter Health Vendor Reports Patient Information Incident* (Nov. 3, 2023), https://vitals.sutterhealth.org/sutter-health-vendor-reports-patient-information-incident/.
[21] *See* Data Breach Notice, **Exhibit A**.

the Internet as part of its contracted services with health plans, including Defendant Sutter Health.

45. On May 31, 2023, Defendant Welltok was notified by Defendant PSC about a vulnerability in the MOVEit software. Welltok applied a patch and mitigations recommended by PSC.[22]

46. Welltok's initial investigation suggested its MOVEit server had not been compromised.[23]

47. On July 26, 2023, Defendant Welltok was alerted about an earlier breach of its MOVEit server. According to Welltok, it "conducted an examination of [its] systems and networks using all information available to determine the potential impact of the vulnerabilities [it was] alerted to on the [Welltok MOVEit server] and the security of data housed on the server, and confirmed that there was no indication of any compromise at that time."[24]

48. On August 11, 2023, after further investigation and "a full reconstruction of [Welltok's] systems and historical data, the investigation determined. .. that an unauthorized actor exploited software vulnerabilities, accessed the [Welltok MOVEit server] on May 30, 2023, and exfiltrated certain data from the [Welltok MOVEit server] during that time."[25]

49. Only after "Welltok subsequently undertook a time-consuming and detailed reconstruction and review of the data stored on the [Welltok MOVEit server]" did Defendant Welltok confirm that the MOVEit vulnerability had been exploited on May 30, 2023, the day before Welltok installed the patch recommended by PSC.[26]

---

[22] Steve Alder, *Welltok Data Breach: 8,493,379 Individuals Affected*, THE HIPAA JOURNAL (Nov. 21, 2023), https://www.hipaajournal.com/welltok-data-breach/.
[23] WELLTOK, *Notice of Data Privacy Event*, https://welltoknotice.wpenginepowered.com/?page_id=23 (last visited Dec. 11, 2023).
[24] *Id.*
[25] *Id.*
[26] *Id.*

50. On August 26, 2023, Welltok finally "learned" that the Private Information belonging to millions of patients had been accessed and exposed by unauthorized threat actors on May 30, 2023.[27]

51. According to the Data Breach Notice that Defendant Welltok posted on its website on October 24, 2023—two months after Welltok claims it finally confirmed that Private Information had been compromised and nearly five months after Welltok was first informed of the MOVEit vulnerability—the affected information included: names, addresses, telephone numbers, email addresses, Social Security numbers, Medicare/Medicaid ID numbers, health insurance information (such as plan or group name), and other health information (such as provider name, prescription name, and treatment codes).[28]

52. Defendant Welltok waited until October 31, 2023 to send a Data Breach Notice letter to Plaintiff Cooper-Leonard.[29]

53. Defendant Welltok waited nearly five months from the date of the Data Breach, and over two months from the date it confirmed the scope of the Data Breach and the highly sensitive nature of the Private Information impacted, to publicly disclose the Data Breach and notify affected individuals.

54. In the aftermath of the Data Breach, Defendant Welltok has not indicated any measures it has taken to mitigate the harm beyond "reviewing and enhancing [its] existing policies and procedures related to data privacy to reduce the likelihood of a similar future event."[30] There is no indication whether these measures are adequate to protect Plaintiff's and Class Members'

---

[27] *Id.*
[28] *See id.*
[29] *See* Data Breach Notice, **Exhibit A**.
[30] WELLTOK, *Notice of Data Privacy Event*, https://welltoknotice.wpenginepowered.com/?page_id=23 (last visited Dec. 11, 2023).

Private Information going forward.

55. According to Defendants Welltok and Sutter Health, Plaintiff's and Class Members' Private Information was exfiltrated and stolen in the Data Breach.

56. The accessed data contained Private Information that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

57. As HIPAA covered business entities that collect, create, and maintain significant volumes of Private Information, the targeted attack was a foreseeable risk which Defendants Welltok, Virgin Pulse, and Sutter Health were aware of and knew they had a duty to guard against. It is well-known that healthcare providers and their business associates such as Defendants, which collect and store the confidential and sensitive Private Information of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

58. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

59. Defendants had obligations created by HIPAA, contract, industry standards, common law, and their own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and protected from unauthorized access and disclosure.

60. Plaintiff and Class Members entrusted Defendants (or their doctors and healthcare providers) with their Private Information with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

61. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew, or should have known, that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

62. Due to Defendants' inadequate security measures and their delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

63. According to published reports, Defendants fell victim to a MOVEit Transfer attack, originating from a zero-day vulnerability and carried out by Russia-linked ransomware syndicate Cl0p.

64. MOVEit Transfer is a managed file transfer software. The zero-day vulnerability affected MOVEit Transfer's servers, allowing attackers to access and download the data stored there, including that of Defendants.

65. Cl0p posted on their dark web blog that they had taken Defendants' data.

66. The Cl0p ransomware gang has taken credit for exploiting the MOVEit zero-day bug. They claim to have breached hundreds of companies in the process.

67. So far, over 2000 organizations have fallen victim to the MOVEit attacks, with the estimated number of exposed individuals exceeding 72 million. Cl0p has been posting victims' names on their dark web leak site since June 14, 2023. The extent of the exposed data depends on how a certain company uses the file transfer system.

68. Cl0p operates under the Ransomware-as-a-Service (RaaS) mode, which means that it rents the software to affiliates for a pre-agreed cut of the ransom payment.

69. Cl0p employs the "double-extortion" technique of stealing and encrypting victim

data, refusing to restore access, and publishing exfiltrated data into its data leak site if the ransom is not paid. On information and belief, Defendants did not pay a ransom to Cl0p.

The Data Breach was a Foreseeable Risk of which Defendants Were on Notice

70. As HIPAA-covered entities handling medical patient data, Defendants Welltok, Virgin Pulse, and Sutter Health's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the Data Breach.

71. At all relevant times, Defendants Welltok, Virgin Pulse, and Sutter Health knew, or should have known that Plaintiff's and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyberattacks that they should have anticipated and guarded against.

72. In light of recent high profile data breaches at other health care providers, Defendants Welltok, Virgin Pulse, and Sutter Health knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

73. Cyber criminals target institutions which collect and store PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company, Protenus, found that there were at least 905 health data breaches in 2021, impacting over 50 million patients. The report noted that "the volume and impact of breaches continue to be underreported overall, and underrepresented to the public[,]" stressing that "gaps in detection and reporting mean

the true impact of incidents is likely even greater."[31]

74. The healthcare sector suffered at least 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[32]

75. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendants Welltok, Virgin Pulse, and Sutter Health knew or should have known that their electronic records would be targeted by cybercriminals.

76. Indeed, cyberattacks against the healthcare industry have been common for over eleven years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII[.]" The FBI further warned that "the increasing sophistication of

[31] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/hubfs/Breach_Barometer/BreachBarometer_Privacy_2022_Protenus.pdf?utm_campaign=Forbes%2520Articles&utm_source=forbes&utm_medium=article&utm_content=breach%2520barometer (last visited Dec. 11, 2023).

[32] *See* Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, HEALTH IT SECURITY: CYBERSECURITY NEWS (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

cyber criminals will no doubt lead to an escalation in cybercrime."[33]

77. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[34] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[35] A study by Experian found that the "average total cost" of medical identity theft was "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[36]

78. In fact, according to the cybersecurity firm Mimecast, 90 percent of healthcare organizations experienced cyberattacks in 2020.[37]

79. Cyberattacks on medical systems have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. .. because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[38]

80. According to an article in the HIPAA Journal posted on November 2, 2023,

---

[33] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[34] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[35] *Id.*

[36] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

[37] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

[38] *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

cybercriminals hack into medical practices for their highly prized medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights (OCR)] – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[39]

81. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[40] In this case, Defendants Welltok, Virgin Pulse, and Sutter Health stored the records of *millions* of patients.

82. Private Information, like that stolen from Defendants Welltok, Virgin Pulse, and Sutter Health, is "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[41]

83. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[39] Steve Alder, *Editorial: Why Do Criminals Target Medical Records*, THE HIPAA JOURNAL (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[40] *See id*.
[41] *See id.*

84. Defendants were on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[42]

85. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[43]

86. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

87. The U.S. Department of Health and Human Services and the Office of Consumer Rights urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines,

---

[42] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820.

[43] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[44]

88. As HIPAA covered entities, Defendants Welltok, Virgin Pulse, and Sutter Health should have known about their data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in their unprotected files.

Defendants Fail to Comply with FTC Guidelines

89. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

90. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[45] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from

[44] Susan D. Hall, *OCR levies $2 million in HIPAA fines for stolen laptops*, Fierce Healthcare (Apr. 23, 2014), https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops.

[45] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

the system; and, have a response plan ready in the event of a breach.[46]

91. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

92. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

93. These FTC enforcement actions include actions against healthcare providers and partners like Defendants. *See, e.g.*, *In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

94. Defendants failed to properly implement basic data security practices.

95. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

96. Defendants were at all times fully aware of their obligations to protect the Private

[46] *Id.*

Information of customers and patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Fail to Comply with Industry Standards

97. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

98. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

99. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

100. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

101. These foregoing frameworks are existing and applicable industry standards in the

healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

Defendants' Conduct Violates
HIPAA Obligations to Safeguard Private Information

102. As healthcare service providers handling medical patient data and providing services to hospitals and healthcare organizations, Defendants Welltok, Virgin Pulse, and Sutter Health are covered entities under HIPAA (45 C.F.R. § 160.103) and are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

103. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

104. Defendants Welltok, Virgin Pulse, and Sutter Health are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

105. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

106. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

107. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the

Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under the authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306 (a)(1-4); 45 C.F.R. § 164.312 (a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308 (a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

108. A Data Breach such as the one Defendants experienced, is considered a breach under the HIPAA Rules because it involved an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40

109. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendants Welltok, Virgin Pulse, and Sutter Health failed to comply with safeguards mandated by HIPAA regulations.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

110. Cyberattacks and data breaches at healthcare service providers like Defendants are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

111. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[47]

[47] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

112. Researchers have further found that for medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes.[48]

113. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[49]

114. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

---

[48] *See* Sung J. Choi, et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), *available at* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[49] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf.

115. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[50]

116. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

117. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

118. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[51]

119. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious

[50] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last visited Dec. 11, 2023).

[51] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

120. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

121. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
>
> GAO Report at 29.

122. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

123. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts, or the accounts of deceased individuals for whom Class Members are the executors or surviving spouses, for many years to come.

124. Private Information can sell for as much as $363 per record according to the Infosec Institute.[52] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

[52] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

125. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[53] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[54] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

126. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

127. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[55]

128. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at the cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[56]

---

[53] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.
[54] *Id*.
[55] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.
[56] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*

129. Medical information is especially valuable to identity thieves.

130. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[57]

131. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

132. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

133. For this reason, Defendants knew or should have known about these dangers and strengthened their data and email handling systems accordingly. Defendants were on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendants failed to properly prepare for that risk.

DEFENDANTS' DATA BREACH

134. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the

Numbers, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[57] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Dec. 11, 2023).

following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. Failing to train their employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the

security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic Private Information they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

135. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Defendants' computer network and systems for multiple days which contained unsecured and unencrypted Private Information.

136. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendants.

Plaintiff's and Class Members' Damages

137. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Defendants have done nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Defendants have not demonstrated any efforts to prevent additional harm from befalling Plaintiff and Class Members as a result of the Data Breach.

138. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

139. Plaintiff's and Class Members' demographic information, dates of birth, Social Security Numbers, and sensitive medical and health information were all compromised in the Data Breach and are now in the hands of the cybercriminals.

140. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

141. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

142. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

143. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

144. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

145. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

146. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiff's and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

147. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

148. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have

recognized the propriety of loss of value damages in similar cases.

149. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendants and/or Defendants' healthcare partners was intended to be used by Defendants to fund adequate security of their computer system(s) and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

150. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

151. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

152. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

153. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

154. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiff's Experience

155. According to the Data Breach Notice letter Plaintiff received from Defendant Welltok, her Private Information was impacted in the Data Breach.[58]

156. Upon information and belief, Plaintiff was presented with standard forms to complete prior to receiving medical services that required her PII and PHI. Upon information and belief, Defendants Welltok, Virgin Pulse, and Sutter Health received and maintain the information

[58] *See* Data Breach Notice, **Exhibit A**.

Plaintiff was required to provide to her doctors or medical professionals. Plaintiff also believes she was presented with standard HIPAA privacy notices before disclosing her Private Information to her medical provider(s).

157. Plaintiff is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

158. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach Notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit.

159. Plaintiff was forced to spend multiple hours attempting to mitigate the effects of the Data Breach. She will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This is time that is lost forever and cannot be recaptured.

160. Plaintiff suffered actual injury and damages from having her Private Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of her Private Information, a form of intangible property that Defendants Welltok, Virgin Pulse, and Sutter Health obtained from Plaintiff and/or Plaintiff's doctors and medical professionals; (b) violation of her privacy rights; (c) the theft of her Private Information; (d) loss of time; (e) imminent and impending injury arising from the increased risk of identity theft and fraud; (f) failure to receive the benefit of her bargain; and (g) nominal and statutory damages.

161. Plaintiff has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff has also suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to her Social Security number, medical records, and prescriptions.

162. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at a present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

163. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

164. Plaintiff brings this action against Defendants individually and on behalf of all other persons similarly situated (the "Class").

165. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Defendants identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

166. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives,

attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

167. Plaintiff reserves the right to amend or modify the Class definition or create additional subclasses as this case progresses.

168. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The U.S. Department of Health and Human Services investigation reports that approximately 8.5 million individuals, including at least 845,000 Sutter Health patients, were impacted by Defendants' Data Breach.[59]

169. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

[59] U.S. Department of Health and Human Services, Currently Under Investigation, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. 11, 2023).

e. Whether Defendants owed a duty to Plaintiff and Class Members to safeguard their Private Information;

f. Whether Defendants breached their duty to Plaintiff and Class Members to safeguard their Private Information;

g. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

h. Whether Defendants should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants breach implied contracts with Plaintiff and Class Members;

l. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

170. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

171. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and

experienced in litigating class actions.

172. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the data of Plaintiff and Class Members was stored on the same network and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

173. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

174. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

175. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

176. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

CLAIMS FOR RELIEF

COUNT I
Negligence

(*On Behalf of Plaintiff and the Class*)

177. Plaintiff re-alleges and incorporates by reference substantive paragraphs as if fully set forth herein.

178. By collecting and storing the Private Information of Plaintiff and Class Members, in their computer systems and networks, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer

systems—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

179. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

180. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of patients that Defendants were aware, or should have been aware, could be injured by inadequate data security measures.

181. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

182. Defendants Welltok, Virgin Pulse, and Sutter Health's duty to use reasonable security measures under HIPAA required them to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

183. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

184. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

185. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;
b. Failing to adequately monitor the security of their networks and systems;
c. Failing to ensure that their email systems had plans in place to maintain reasonable data security safeguards;
d. Failing to have in place mitigation policies and procedures;
e. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;
f. Failing to detect in a timely manner that Plaintiff's and Class Members' Private Information had been compromised; and
g. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft

and other damages.

186. Plaintiff and Class Members have no ability to protect their Private Information that was or remains in Defendants' possession.

187. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

188. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in one or more types of injuries to Plaintiff and Class Members. In addition, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

189. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information, and failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

190. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

191. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

192. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known

that they were failing to meet their duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

193. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract

(On behalf of Plaintiff and the Class)

194. Plaintiff re-alleges and incorporates by reference substantive paragraphs as if fully set forth herein.

195. Defendants acquired and maintained the Private Information of Plaintiff and the Class that they received either directly or from their healthcare providers.

196. When Plaintiff and Class Members paid money and provided their Private Information to their doctors and/or healthcare providers, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with their doctors and/or healthcare professionals, their business associates, revenue service providers, and file transfer software providers, including Defendants.

197. Plaintiff and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

198. Plaintiff and the Class were required to deliver their Private Information to Defendants as part of the process of obtaining services provided by Defendants. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for services.

199. Defendants Welltok, Virgin Pulse, and Sutter Health solicited, offered, and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants, or, alternatively, provided their information to doctors or other healthcare professionals, who then provided it to Defendants. In turn, Defendants Welltok, Virgin Pulse, and Sutter Health provided that same Private Information to Defendant PSC in the course of using Defendant PSC's MOVEit software.

200. Defendants accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members and/or their doctors and other healthcare professionals.

201. In accepting such information and payment for services, Defendants entered into implied contracts with Plaintiff and Class Members whereby Defendants became obligated to reasonably safeguard Plaintiff's and Class Members' Private Information.

202. Alternatively, Plaintiff and Class Members were the intended beneficiaries of data protection agreements entered into between Defendants and healthcare providers.

203. In delivering, directly or indirectly, their Private Information to Defendants and paying for healthcare services, Plaintiff and Class Members intended and understood that Defendants would adequately safeguard the data as part of that service.

204. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

205. The implied promises include but are not limited to: (1) taking steps to ensure that

any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

206. Plaintiff and Class Members (or their doctors and healthcare providers) would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

207. Had Defendants disclosed to Plaintiff and Class Members (or their doctors and healthcare providers) that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members (or their doctors and healthcare providers) would not have provided their Private Information to Defendants.

208. Defendants recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members (or their doctors and healthcare providers).

209. Plaintiff and Class Members (or their doctors and healthcare providers) fully performed their obligations under the implied contracts with Defendants.

210. Defendants breached the implied contracts with Plaintiff and Class Members (or their doctors and healthcare providers) by failing to take reasonable measures to safeguard their Private Information as described herein.

211. As a direct and proximate result of Defendants' conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III
Unjust Enrichment

(On Behalf of Plaintiff and the Class)

212. Plaintiff re-alleges and incorporates by reference substantive paragraphs as if fully set forth herein.

213. This count is pleaded in the alternative to breach of contract.

214. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including from money they make based upon protecting Plaintiff's and Class Members' Private Information.

215. There is a direct nexus between money paid to Defendants and the requirement that Defendants keep Plaintiff's and Class Members' Private Information confidential and protected.

216. Plaintiff and Class Members paid Defendants and/or healthcare providers a certain sum of money, which was used to fund data security via contracts with Defendants.

217. As such, a portion of the payments made by or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

218. Protecting the Private Information of Plaintiff and Class Members is integral to Defendants' businesses. Without their data, Defendants Welltok, Virgin Pulse, and Sutter Health would be unable to provide the services to hospital and healthcare providers comprising Defendants' core businesses, and Defendant PSC would be unable to provide the software services comprising Defendant PSC's core business.

219. Plaintiff's and Class Members' data and Private Information has monetary value.

220. Plaintiff and Class Members directly and indirectly conferred a monetary benefit on Defendants. They indirectly conferred a monetary benefit on Defendants by purchasing goods

and/or services from entities that contracted with Defendants, and from which Defendants received compensation to protect certain data. Plaintiff and Class Members directly conferred a monetary benefit on Defendants by supplying Private Information, which has value, from which value Defendants derive their business value, and which should have been protected with adequate data security.

221. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

222. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failures to provide the requisite security.

223. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

224. Defendants acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

225. If Plaintiff and Class Members knew that Defendants had not secured their Private

Information, they would not have agreed to provide their Private Information to Defendants (or to their physician to provide to Defendants).

226. Plaintiff and Class Members have no adequate remedy at law.

227. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; (vii) loss or privacy from the authorized access and exfiltration of their Private Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

228. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

229. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and

Class Members overpaid for Defendants' services.

COUNT IV
Bailment

(*On Behalf of Plaintiff and the Class*)

230. Plaintiff re-alleges and incorporates by reference substantive paragraphs as if fully set forth herein.

231. Plaintiff and Class Members provided Private Information to Defendants—either directly or through healthcare providers and their business associates—which Defendants were under a duty to keep private and confidential.

232. Plaintiff's and Class Members' Private Information is personal property, and was conveyed to Defendants for the certain purpose of keeping the information private and confidential.

233. Plaintiff's and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendants were aware of the risks they took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

234. Once Defendants accepted Plaintiff's and Class Members' Private Information, they were in the exclusive possession of that information, and neither Plaintiff nor Class Members could control that information once it was within the possession, custody, and control of Defendants.

235. Defendants did not safeguard Plaintiff's or Class Members' Private Information when they failed to adopt and enforce adequate security safeguards to prevent the known risk of a cyberattack.

236. Defendants' failure to safeguard Plaintiff's and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

237. As a result of Defendants' failure to keep Plaintiff's and Class Members' Private Information secure, Plaintiff and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

COUNT V
Breach of Fiduciary Duty

(On Behalf of Plaintiff and the Class)

238. Plaintiff re-alleges and incorporates by reference substantive paragraphs as if fully set forth herein.

239. In light of the special relationship between Defendants and Plaintiff and Class Members, Defendants became fiduciaries by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants do store.

240. Defendants had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship with patients (or the patients of their healthcare clients), in particular, to keep secure their Private Information.

241. Defendants breached their fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

242. Defendants breached their fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

243. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i)

actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendants' services they received.

244. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class Action and appointing Plaintiff as Class Representative and her counsel as Class Counsel;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendants to utilize appropriate methods and

policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, nominal damages, and/or statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) Pre- and post-judgment interest on any amounts awarded; and,

i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: December 12, 2023

Respectfully submitted,

/s/ Steven B. Rotman
Steven B. Rotman (MA Bar No. 558473)
HAUSFELD LLP
One Marina Park Drive, Suite 1410
Boston, MA 02210
Tel.: (617) 207-0600
Fax: (617) 830-8312
Email: srotman@hausfeld.com

James J. Pizzirusso
HAUSFELD LLP
888 16th Street, N.W., Suite 300
Washington, D.C. 20006
Tel.: (202) 540-7200
Fax: (202) 540-7201
Email: jpizzirusso@hausfeld.com

Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street, Fourteenth Floor
New York, NY 10004
Tel.: (646) 357-1100
Fax: (212) 202-4322
Email: snathan@hausfeld.com

Counsel for Plaintiff